REMARKS

CLAIMS:

Claims 1-50 comprise the case.

I) 35 U.S.C. 102

Claims 1, 8-9, 14-15, 22-23, 28-29, 35, 39-40, 46 and 50 have been rejected as being unpatentable over Anderl et al. (Int. Publication WO 87/07062) under 35 U.S.C. 102(b):

A) Claim 1:

As to independent Claim 1, the Examiner states "Anderl et al. teaches a portable security system for managing access to a portable data storage cartridge *** comprising: a wireless interface ***; and a computer processor ***; the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct *** (see page 11, lines 14-26, where 'user identifier' is read on 'login level'), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user ***, the computer processor receiving the user authentication messages from the data storage drive ***, combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity, ***." (emphasis added).

1) Applicant respectfully submits that the "login level" of Anderl et al. does not read on Applicant's "user identifier", which comprises, e.g., Claim 1, "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media". (emphasis added).

As pointed out by the accompanying Second Declaration under Rule 1.132, in Anderl et al., "'Security for the card is provided by requiring a separate password for gaining access to each of designated levels of interaction between the card and the associated station.' ***.

"That, a fundamental distinguishing difference exists between the 'designated levels of interaction' of Anderl et al. and the present '899 Application's 'at least one unique user identifier for each authorized user'. ***.

"To base an argument on Anderl et al., regardless of the actual number of users, there would be only ONE user at any given access level, or login level. To equate 'user' with 'login level' requires that all 'users' of a particular characteristic (in Anderl et al.) are indistinguishable. ***.

"In contrast, access characteristics are defined with respect to 'each authorized user' in the present '899 Application.

"In the present '899 Application, the access characteristics are part of the user table, allowing a many/many relationship where access privilege follows the user by means of the 'user table comprising at least one unique user identifier for each authorized user'. ***"

Hence, Applicant respectfully submits that Claim 1 is patentable over Anderl et al.

2) Further, Applicant respectfully submits that the user authentication (for each user) of Claim 1 patentably defines over the password of Anderl et al. Claim 1 recites user

authentication "combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity". (emphasis added).

As pointed out by the accompanying Second Declaration under Rule 1.132, "Anderl et al. requires that a login specify the level and password as a specific request. ***.

"In contrast, in the present '899 Application, access permissions of the user table are separate from the authentication method. The user table comprises 'at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.' ***."

Hence, Applicant further respectfully submits that Claim 1 is patentable over Anderl et al.

3) Still further Applicant respectfully submits that the individual association of each user and the user's permitted activity defined by Claim 1 patentably defines over Anderl et al. Claim 1 recites "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media". (emphasis added).

As pointed out by the accompanying Second Declaration under Rule 1.132, "Anderl et al. relies on a fixed relationship between all login levels (i.e., the password may be changed for levels lower than the currently logged in level). ***.

"In contrast, again, access characteristics are defined with respect to 'each authorized user' in the present '899 Application.

"In the present '899 Application, the access characteristics are part of the user table, allowing a many/many relationship where access privilege follows the user by means of the 'user table comprising at least one unique user identifier for each authorized user'. ***."

Hence, Applicant further respectfully submits that Claim 1 is patentable over Anderl et al.

B) Claims 15, 29 and 40:

The Examiner rejected independent Claims 15, 29 and 40 as being unpatentable over Anderl et al. in the same manner as independent Claim 1, above, reading "user identifier" of the respective claim on "login level" of Anderl et al.

Applicant respectfully submits that the "login level" of Anderl et al. does not read on Applicant's "user identifier" of Claims 15, 29 or 40, which comprises, e.g., Claim 15, "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct". (emphasis added).

Thus, as pointed out above with respect to Claim 1, Applicant's Claims 15, 29 and 40 are submitted to define access characteristics with respect to 'each authorized user' and to thereby patentably define over the "login level" of Anderl in which all "users" of a particular characteristic are indistinguishable."

Additionally, Applicant respectfully submits that the user authentication (for each user) of Claims 15, 29 and 40 patentably define over the password of Anderl et al., as discussed above with respect to Claim 1. For example, Claim 15 recites user authentication "combining said user authentication message with said user identifier from said user table in accordance with said

predetermined algorithm to authorize or deny said user activity". (emphasis added).

Still further Applicant respectfully submits that the individual association of each user and the user's permitted activity defined by Claims 15, 29 and 40 patentably defines over Anderl et al., also as discussed above with respect to Claim 1. For example Claim 15 recites "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media". (emphasis added).

Hence, Applicant respectfully submits that independent Claims 15, 29 and 40 patentably define over Anderl et al.

C) Claims 8, 22 and 46:

The Examiner states that Anderl et al. teaches that the "user table comprises a separate entry for each the user identifier, the entry comprising all the permitted activities the user is authorized to conduct".

Applicant respectfully submits that, as discussed above, Anderl et al. security is based on designated levels of interaction between the card and the associated station without regard to the number of actual users at each level.

As pointed out by the accompanying Second Declaration under Rule 1.132, "In contrast, again, access characteristics are defined with respect to 'each authorized user' in the present '899 Application."

Thus, Applicant respectfully submits that Claims 8, 22 and 46 patentably define over Anderl et al., e.g. Claim 8 reciting "said computer processor user table comprises a separate entry for each said user identifier, said entry comprising all said

permitted activities said user is authorized to conduct." (emphasis added).

D) Claims 9 and 23:

The Examiner states that Anderl et al. teaches a "nonvolatile memory storing the user table (see page 11, lines 21-26)."

Applicant respectfully submits that the "table" of Anderl et al. comprises "passwords for each security level are placed in the card header", and relate to designated levels of interaction between the card and the associated station without regard to the number of actual users at each level, as discussed above.

As pointed out above, in contrast, the "user table" of Claims 9 and 23 is defined as "comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct" in respectively Claims 1 and 15, from which Claims 9 and 23 depend.

Thus, Applicant respectfully submits that Claims 9 and 23 patentably define over Anderl et al.

E) Claims 14, 28, 39 and 50:

The Examiner states that Anderl et al. teaches encrypted data and wherein the "user table permitted activities comprise at least 1) read access to data *** and wherein the user authorization for the read access additionally comprises a decryption key *** (page 2, lines 20-23, where it is inherent that user authorization would have to comprise a decryption key if the data was encrypted)."

Applicant respectfully submits that, as discussed above, Anderl et al. fails to disclose a "user table" as defined by

Claims 1, 15, 29 or 40, from which Claims 14, 28, 39 and 50 depend. Further, Applicant respectfully submits that the "encrypted data" referred to in Anderl et al. comprises "encryption of data as it is provided to the card is also available" and appears unrelated to the card login levels and password control. (page 2, lines 21-22). (emphasis added).

Hence, Applicant respectfully submits that Claims 14, 28, 39 and 50, e.g. Claim 14, define "wherein said computer processor user table permitted activities comprise at least 1) read access to data stored in said data storage media, and wherein said user authorization for said read access additionally comprises a decryption key for said encrypted stored data", and thereby patentably define over Anderl et al.

F) Claim 35:

The Examiner states that Anderl et al. shows a user table with "a separate entry for each the user identifier, *** wherein the transmitting step additionally comprises identifying the user permitted activities from the user separate entry".

Applicant respectfully submits that the "table" of Anderl et al. relates to designated levels of interaction between the card and the associated station without regard to the number of actual users at each level, as discussed above.

As pointed out above, in contrast, the "user table" of Claim 29, from which Claim 35 depends, is defined as "comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct", and that Claim 35 recites "wherein said step of providing said user table comprises a separate entry for each said user identifier, said entry comprising all said permitted activities said user is authorized to conduct; and wherein said transmitting

step additionally comprises identifying said user permitted activities from said user separate entry."

Hence, Applicant respectfully submits that Claim 35 patentably defines over Anderl et al.

SUMMARY:

Applicant respectfully submits that Claims 1, 8-9, 14-15, 22-23, 28-29, 35, 39-40, 46 and 50 are therefore patentable over Anderl et al. under 35 U.S.C. 102(b), and respectfully requests allowance thereof.

II) 35 U.S.C. 103

G) Claims 2 and 16:

Claims 2 and 16 have been rejected as being unpatentable over Anderl et al. in view of Davis (U.S. Patent No. 4,941,201) under 35 U.S.C. 103(a):

The Examiner states that Anderl et al. "does not teach wherein the wireless interface comprises an RF interface." Davis is said to teach "an RF interface". The Examiner further states "it would have been obvious *** to have modified Anderl et al. to include *** an RF interface. *** by the teachings of Davis ***".

Applicant respectfully submits, that as pointed out by the first Declaration under Rule 1.132, Davis "relates to an 'electronic data storage *** apparatus *** wherein a combination power and data signal is received by a preferably portable *** data storage means ***'. *** Davis shows a data storage device with CMOS logic that stores and addresses data, without any user authentication. *** Davis shows an address-like initialization access code to address a particular memory location of the

device, but shows nothing directed to a user identifier. *** Davis shows an address-like initialization access code to address a particular memory location of the device, but shows no user authentication or decryption. *** Davis has no ability to manage access."

Applicant therefore respectfully submits that the frequency of the Davis communication signal is not relevant to Applicant's Claims 2 and 16, which depend respectively from Claims 1 and 15, and which define, e.g. Claim 1, "said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface."

Further, Davis is submitted to be unable to make up for the failings of Anderl et al. as discussed above.

Hence, Applicant respectfully submits that Applicant's Claims 2 and 16 are therefore patentable over Anderl et al. and Davis under 35 U.S.C. 103(a).

III) 35 U.S.C. 103

Claims 3-5, 17-19, 30-32 and 41-43 have been rejected as being unpatentable over Anderl et al. in view of Ichikawa (U.S. Patent No. 5,872,846) under 35 U.S.C. 103(a):

H) Claims 3, 17, 30 and 41:

The Examiner states that Anderl et al. teaches a "user identifier" that "comprises a user symbol and a user decrypting key *** where 'user symbol' is read on 'login level' and 'decrypting key' is read on 'password'". The Examiner states

that Anderl et al. does not teach "an encrypted user authentication message *** wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key." Ichikawa is said to teach such an authentication message, and "it would have been obvious *** to have modified Anderl et al. to include wherein the user authentication message comprises an encrypted user authentication message" etc., using the teaching of Ichikawa.

Applicant respectfully submits that Ichikawa instead provides a "system and method for providing security in data communication systems where multiple users are coupled to a common receiving system. *** The transmitted data is received at a receiver where it is descrambled or otherwise decoded." (Abstract, lines 1-7).

Applicant's Claims 3, 17, 30 and 41 depend respectively from Claims 1, 15, 29 and 40.

As discussed above, Applicant respectfully submits that the "login level" of Anderl et al. does not read on Applicant's "user identifier" of Claims 1, 15, 29 or 40, which comprises, e.g., Claim 1, "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct". (emphasis added).

Thus, as pointed out above, Applicant's Claims 1, 15, 29 and 40 are submitted to define access characteristics with respect to 'each authorized user' and to thereby patentably define over the "login level" of Anderl in which all "users" of a particular characteristic are indistinguishable."

Additionally, Applicant respectfully submits that the user authentication (for each user) of Claims 1, 15, 29 and 40 patentably define over the password of Anderl et al., as discussed above with respect to Claim 1. For example, Claim 1 recites user authentication "combining said user authentication message with said user identifier from said user table in

accordance with said predetermined algorithm to authorize or deny said user activity". (emphasis added).

Still further Applicant respectfully submits that the individual association of each user and the user's permitted activity defined by Claims 1, 15, 29 and 40 patentably defines over Anderl et al., also as discussed above. For example Claim 1 recites "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media". (emphasis added).

Hence, Applicant respectfully submits that Anderl et al. fails to show or suggest a "user authentication message" to be combined "with said user identifier from said user table" of Claims 1, 15, 29 and 40 in accordance with Claims 3, 17, 30 and 41, and that the decryption of Ichikawa adds nothing to Anderl et al. to provide such a user authentication message. Referring for example to Claim 3, Applicant respectfully submits that the recitation "wherein each said user identifier comprises a user symbol and a user decrypting key, wherein said user authentication message comprises an encrypted user authentication message which may be decrypted by said user decrypting key, and wherein said computer processor conducts said combination by decrypting said user authentication message by said user decrypting key" patentably defines over Anderl et al. and Ichikawa.

Applicant therefore respectfully submits that Claims 3, 17, 30 and 41 are patentable over Anderl et al. and Ichikawa under 35 U.S.C. 103(a).

I) Claims 4, 18, 31 and 42:

The Examiner stated that Anderl et al. as modified by Ichikawa teaches "the user decrypting key comprises a sender public key ***".

Applicant respectfully submits that the type of decrypting key of Ichikawa relates only to data communication, and, as discussed above, fails to provide such a user authentication message, as is recited in Claims 1, 15, 29 and 40 in accordance with Claims 4, 18, 31 and 42.

Applicant therefore respectfully submits that Claims 4, 18, 31 and 42 are patentable over Anderl et al. and Ichikawa under 35 U.S.C. 103(a).

J) Claims 5 and 19:

The Examiner stated that Anderl et al. as modified by Ichikawa teaches "the user authentication message is encrypted by a sender private key and a receiver public key ***".

Applicant respectfully submits that the type of decrypting key of Ichikawa relates only to data communication, and, as discussed above, fails to provide such a user authentication message, as is recited in Claims 1 and 15 in accordance with Claims 5 and 19.

Applicant therefore respectfully submits that Claims 5 and 19 are patentable over Anderl et al. and Ichikawa under 35 U.S.C. 103(a).

K) Claims 32 and 43:

The Examiner stated that Anderl et al. as modified by Ichikawa teaches "the user authentication message is encrypted by

a sender private key and a receiver public key, *** and wherein the combining step comprises decrypting the user authentication message by the receiver private key and the sender public key ***".

Applicant respectfully submits that the type of decrypting key of Ichikawa relates only to data communication, and, as discussed above, fails to provide such a user authentication message, as is recited in Claims 29 and 40 in accordance with Claims 32 and 43.

Applicant therefore respectfully submits that Claims 32 and 43 are patentable over Anderl et al. and Ichikawa under 35 U.S.C. 103(a).

SUMMARY:

Applicant respectfully submits that Claims 3-5, 17-19, 30-32 and 41-43 are therefore patentable over Anderl et al. and Ichikawa under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

IV) 35 U.S.C. 103

Claims 6-7, 10-13, 20-21, 24-27, 33-34, 36-38, 44-45 and 47-49 have been rejected as being unpatentable over Anderl et al. in view of Bapat et al. (U.S. Patent No. 6,038,563) under 35 U.S.C. 103(a):

L) Claims 6, 20 and 44:

The Examiner states that Anderl et al. teaches that "user table permitted activities comprise a plurality of permitted activities" including "1) read access to data stored in the data storage media, 2) write access to data stored in the data storage

media", but not activities related to reading and modifying the user table itself, but that Bapat et al. does. "It would have been obvious *** to have modified Anderl et al. to include the permitted activities comprising 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table. and 6) change/delete entries to the user table", the modification by the teachings of Bapat et al.

Anderl et al. has been discussed above where Applicant respectfully submits that the "login level" of Anderl et al. does not read on Applicant's "user identifier", such that Anderl et al. fails to provide, e.g., Claim 1, "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct" of Claims 1, 15 or 40, from which Claims 6, 20 and 44 depend. (emphasis added).

Bapat et al. relates to a computer network, and shows an "access control database has access control objects that collectively store information that specifies access rights by users to specified sets of the managed objects. The specified access rights include access rights to obtain management information from the network." (column 3, lines 17-21). "An access control procedure limits access to the management information stored in the database tables using at least one permissions table." (column 3, lines 32-35) (emphasis added). "Each 'rule' in the access control tree either grants or denies access by certain groups of users *** to a set of target objects". (column 11, lines 4-6).

However, no "user" has access to the "permissions table" to, e.g., Claim 6, "3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table".

Rather, in Bapat et al., a "database access engine *** using the permissions table such that each user is allowed access only

to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46).

Applicant therefore respectfully submits that Claims 6, 20 and 44 are patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

M) Claims 7, 21 and 45:

The Examiner states that, as to Claims 7, 21 and 45, Anderl et al. does not teach a "user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct", which is said to be taught by Bapat et al., and it "would have been obvious *** to have modified Anderl et al." by the teachings of Bapat et al.

Applicant respectfully submits that, as discussed above with respect to Claims 1, 15 or 40, from which Claims 7, 21 and 45 depend, and as pointed out by the accompanying Second Declaration under Rule 1.132, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication.

"In contrast, in the present '899 Application, access permissions of the user table are separate from the authentication method. The user table comprises 'at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.' ***."

Bapat et al. provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the

user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 7, 21 and 45 are patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

N) Claims 10, 24, 36 and 47:

With respect to Claims 10, 24, 36 and 47, the Examiner states that Anderl et al. does not teach "a class table", but that Bapat et al. does teach a "class table comprising at least a unique class identifier for each authorized class of users ***, when combined with a user authentication message from a user of the authorized class of users ***, authorizes the user ***", and that it "would have been obvious *** to have modified Anderl et al. by the teachings of Bapat et al."

Again, as discussed above, Applicant respectfully submits that, with respect to Claims 1, 15, 29 or 40, from which Claims 10, 24, 36 and 47 depend, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication.

Bapat et al. provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier

for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 10, 24, 36 and 47 are patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

O) Claims 11, 25, 37 and 48:

With respect to Claims 11, 25, 37 and 48, the Examiner states that Anderl et al. as modified by Bapat et al. teaches that the "user table additionally comprises any class membership of each the user".

Again, as discussed above, Applicant respectfully submits that, with respect to Claims 1, 15, 29 or 40, from which Claims 11, 25, 37 and 48 depend, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication.

Bapat et al. provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 11, 25, 37 and 48 are patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

P) Claims 12, 26 and 49:

With respect to Claims 12, 26 and 49, the Examiner states that Anderl et al. as modified by Bapat et al. teaches that the "user table and the class table permitted activities" include "3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table".

Again, as discussed above, Applicant respectfully submits that, with respect to Claims 1, 15 or 40, from which Claims 12, 26 and 49 depend, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication. Further, Bapat et al. does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Additionally, Applicant respectfully submits that, in Bapat et al., as discussed above, the permissions table is used to grant access to a database, and further submits that no "user" has access to the "permissions table", to, e.g., Claim 12, "3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table."

Applicant therefore respectfully submits that Claims 12, 26 and 49 are patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

Q) Claims 13 and 27:

With respect to Claims 13 and 27, the Examiner states that Anderl et al. as modified by Bapat et al. teaches a "nonvolatile memory storing the user table".

Applicant respectfully submits that the "table" of Anderl et al. comprises "passwords for each security level are placed in the card header", and relate to designated levels of interaction between the card and the associated station without regard to the number of actual users at each level, as discussed above. Further, Bapat et al. "stores a full copy of the access control object tree" (column 7, lines 18-19) but does not provide a user identifier for authentication, e.g. of Claim 1, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claims 13 and 27, which depend from Claims 1 and 15, are patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

R) Claim 33:

With respect to Claim 33, the Examiner states that Anderl et al. does not teach activities related to reading and modifying the user table itself, but that Bapat et al. does. "It would have been obvious *** to have modified Anderl et al. to include the permitted activities comprising 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table. and 6) change/delete entries to the user table", the modification by the teachings of Bapat et al.

Applicant respectfully submits that Anderl et al. fails to provide, e.g., Claim 29, from which Claim 33 depends, "a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct". (emphasis added). Applicant further submits that Bapat et al. relates to a computer network, and, as discussed above, no "user" has access to the "permissions table" to, e.g., Claim 33, "3) read the user entry of said user table, 4) read all entries of said user table, 5) add entries to said user table, and 6) change/delete entries to said user table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user permitted activities said user is authorized to conduct."

Applicant therefore respectfully submits that Claim 33 is patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

S) Claim 34:

The Examiner states that, as to Claim 34, Anderl et al. does not teach a "user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct", which is said to be taught by Bapat et al., and it "would have been obvious *** to have modified Anderl et al." by the teachings of Bapat et al.

Applicant respectfully submits that, as discussed above with respect to Claim 29, from which Claims 34 depends, and as pointed out by the accompanying Second Declaration under Rule 1.132, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password authentication.

"In contrast, in the present '899 Application, access permissions of the user table are separate from the

authentication method. The user table comprises 'at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user.' ***."

Bapat et al. provides a "database access engine *** using the permissions table such that each user is allowed access only to management information in the set of database tables that the user would be allowed by the access control database to access." (column 3, lines 42-46), and does not provide a user identifier for authentication, e.g. of Claim 29, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Applicant therefore respectfully submits that Claim 34 is patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

T) Claim 38:

With respect to Claim 38, the Examiner states that Anderl et al. as modified by Bapat et al. teaches that the "user table and the class table permitted activities" include "3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table".

Again, as discussed above, Applicant respectfully submits that, with respect to Claim 29, from which Claim 38 depends, Anderl et al. fails to show a user identifier that is used in the authentication. Rather, Anderl et al. has a password

authentication. Further, Bapat et al. does not provide a user identifier for authentication, e.g. of Claim 29, "a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Additionally, Applicant respectfully submits that, in Bapat et al., as discussed above, the permissions table is used to grant access to a database, and further submits that no "user" has access to the "permissions table", to, e.g., Claim 38, "3) read all entries of said class table, 4) add entries to said class table, and 5) change/delete entries to said class table; and wherein said transmitting step comprises transmitting authorization to conduct the selected said user and said class permitted activities said user is authorized to conduct."

Applicant therefore respectfully submits that Claim 38 is patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a).

SUMMARY:

Applicant respectfully submits that Claims 6-7, 10-13, 20-21, 24-27, 33-34, 36-38, 44-45 and 47-49 are therefore patentable over Anderl et al. and Bapat et al. under 35 U.S.C. 103(a), and respectfully requests allowance thereof.

SUMMARY:

Applicant respectfully submits that the present invention distinguishes over the cited patents and respectfully requests that the Examiner allow Applicant's Claims 1-50 under 35 U.S.C. 103.

Respectfully submitted,
P. J. Seger

By: _____
John H. Holcombe, (#20,620)
Attorney for Applicants

From: IBM Corporation
Intellectual Property Law
8987 E. Tanque Verde Rd. #309-374
Tucson, AZ 85749-9610
Telephone: (520) 760-6629

JHH/cw
Attachments: Second Declaration